ABSTRACT OF THE DISCLOSURE

In a distributed digital signature generation method, the method includes the steps of: generating partial signature keys by distributed processes, generating partial digital signatures by using the partial signature keys for the hash value of an input digital document to which additional information such as time is added, combining a predetermined threshold number of partial digital signatures, performing a transformation process on the partial digital signatures according to the combination, and generating an integrated digital signature from the result of the transformation process, in which a least common multiple of predetermined values is used as a transformation number, and it is judged whether an incorrect partial digital signature exists and the number is one, and the incorrect partial digital signature is identified when the number is one.